(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002023627 A

(43) Date of publication of application: 23.01.02

(51) Int. Cl G09C 1/00
G06F 17/60

(21) Application number: 2000200557

(22) Date of filing: 03.07.00

(71) Applicant: NIPPON TELEGR & TELEPH CORP <NTT>

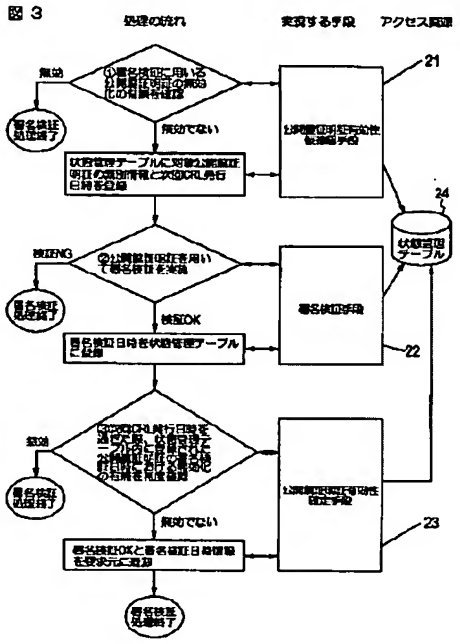
(72) Inventor: HASHIMOTO SHOICHI
MASAMOTO HIROSHI

(54) DEVICE AND METHOD FOR VERIFYING SIGNATURE

(57) Abstract:

PROBLEM TO BE SOLVED: To confirm that a public key certificate used for the verification is surely not invalid at the time of verifying a signature.

SOLUTION: This device (1) confirms that the public key certificate to be used for verifying a signature is not invalidated; (2) verifies the signature by using the public key, and registers the public key certificate identification information, the date of issue of the next CRL (invalidated public key certificate list), and the date of the signature verification in a state management table according to each processing number; and (3) when the next CRL issue date has passed, the device confirms that each certificate identification information was not invalidated on the date when each information was used for the signature verification.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－23627
（P2002－23627A）
(43)公開日　平成14年１月23日(2002.1.23)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ　５Ｂ０４９
			６４０Ｚ　５Ｊ１０４
Ｇ０６Ｆ　17/60	１４０	Ｇ０６Ｆ　17/60	１４０
	５１２		５１２

審査請求　有　　請求項の数２　ＯＬ　（全９頁）

(21)出願番号　特願2000－200557(P2000－200557)

(22)出願日　平成12年７月３日(2000.7.3)

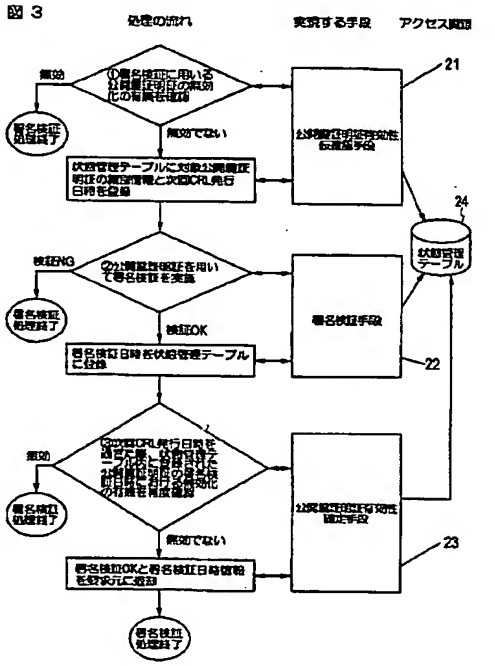
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　橋本　正一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　政本　廣志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　署名検証装置及び署名検証方法

(57)【要約】
【課題】　署名検証した時点でその検証に用いた公開鍵証明証が確かに無効とされてないものであることを確認可能とする。
【解決手段】　①署名検証に用いる公開鍵証明証が無効化されていないことを確認し、②その公開鍵を用いて署名検証を行い、その公開鍵証明証識別情報、次回ＣＲＬ（無効公開鍵証明証リスト）発行日時、署名検証日時を状態管理テーブル２４に各処理番号ごとに登録し、③次回ＣＲＬ発行日時が過ぎると、状態管理テーブル２４内の各証明証識別情報について、それがその署名検証に用いた日時に無効でなかったことを確認し、そのことを検証要求元へ通知する。

図３



【特許請求の範囲】

【請求項１】　処理識別子ごとに署名検証日時、公開鍵証明証識別情報、次回ＣＲＬ（無効化公開鍵証明証リスト）発行日が記憶される状態管理テーブルと、

公開鍵証明証を用いて入力された情報について署名検証処理を行い、上記状態管理テーブルに署名検証を行った日時を登録する署名検証手段と、

署名検証処理時に、これに用いる公開鍵証明証の無効化の有無を確認し、上記状態管理テーブルに確認対象の公開鍵証明証の識別情報と次回ＣＲＬ発行日時を登録する公開鍵証明証有効性仮確認手段と、

次回ＣＲＬ発行日時が過ぎると、上記状態管理テーブル内に登録された識別情報に対応する公開鍵証明証による署名検証日時の時点におけるその公開鍵証明証の無効化の有無を確認する公開鍵証明証有効性確定手段と、を具備することを特徴とする署名検証装置。

【請求項２】　署名検証要求を受け付けると、公開鍵証明証有効性仮確認手段を用いて、署名検証に用いる公開鍵証明証の無効化の有無を確認し、

無効化されていない場合に、対象公開鍵証明証の識別情報と次回ＣＲＬ発行日時を状態管理テーブルに記憶登録し、

続いて上記署名検証要求された情報について上記公開鍵証明証を用いる署名検証処理を行い、

その検証に合格すると、上記状態管理テーブルに署名検証日時を記憶登録し、

現時刻が次回ＣＲＬ発行日時を過ぎると、上記状態管理テーブル内の情報を読み出し、登録された識別情報に対応する公開鍵証明証が、その署名検証日時の時点で無効化されていなかったか否かを確認し、無効化されていなかったことが確認されると、署名検証合格とともに署名検証日時情報を上記署名検証要求元に通知することを特徴とする署名検証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電子データの正当性を確認する際に行う電子署名を検証するための装置及びその方法に関するものである。

【０００２】

【従来の技術】公開鍵暗号を用いた電子署名技術により、利用者の本人確認や通信路における改竄（かいざん）の有無の確認を行うシステムでは、ＣＡ（Certification Authority:認証局）が発行する公開鍵証明証を用いて、電子署名の検証が行われる。公開鍵証明証には、信頼性を低下させないために、利用可能な有効期間が定められているが、公開鍵に対応する秘密鍵の漏洩や、所有者の身元情報に変更が生じるなどの理由により、有効期間内であってもＣＡが残りの有効期間内の効力を強制的に無効化する場合がある。このため、電子署名を検証する際には、公開鍵証明証がＣＡによって無効化されていないことを確認してその公開鍵を利用する必要がある。一般にＣＡは、利用者からの公開鍵証明証の無効化依頼を受け付けると、ＣＲＬ（Certificate Revocation List:証明書取消リスト）と呼ばれる無効化された公開鍵証明証識別情報の一覧を定期的に発行して、外部の利用者に無効化された公開鍵証明証の情報を周知させる。そこで図８に示すように署名検証装置１１ではＣＡ１２から定期的に発行されるＣＲＬをＣＲＬ取得手段１３により取得してＣＲＬ記憶部１４に記憶しておく。署名検証処理部１５で署名検証を行う場合はまずＣＲＬ検索手段１６により、その検証に用いる公開鍵証明証識別情報が、ＣＲＬリストにあるかをＣＲＬ記憶部１４を検索し、ＣＲＬリストにないことつまり対象公開鍵証明証が無効化されていないことを確認して、その公開鍵を用いて、署名検証処理を行う。

【０００３】また、このＣＲＬをＣＡから取得し、公開鍵証明証の無効化の有無の確認を代行する機関であるＶＡ（Validation Authority：検証局）を設けて、ここへの問い合わせにより、対象公開鍵証明証が無効化されていないことを確認する方法もある。つまり図９に示すように、検証局１８ではＣＡから定期的に発行されるＣＲＬを取得記憶しておき、署名検証装置１１で署名検証を行う場合、まずＶＡ問い合わせ手段１９により対象公開鍵証明証の識別情報を検証局１８へ送り、その証明証が有効か否かの問い合わせを行い、検証局１８はその証明証識別情報により、ＣＲＬ記憶部を検索して、なければ有効であること、あれば無効であることを問い合わせのあった署名検証装置１１へ返送する。署名検証装置１１は有効の回答があると、その公開鍵証明証の公開鍵を用いて検証処理を行う。

【０００４】

【発明が解決しようとする課題】上記に示したＣＲＬは、ＣＡによって定期的に発行されるため、一度最新のＣＲＬが発行されると、その発行の後でＣＡに無効化申請された公開鍵証明証の識別情報は、次回に発行されるＣＲＬに掲載されることになり、それが発行されるまで、ＣＡ外部の利用者は無効化された公開鍵証明証の最新情報を知ることができない。したがって、署名検証に用いる公開鍵証明証の無効化の有無をＣＲＬを用いて確認する場合、署名検証時において最新のＣＲＬに確認対象の公開鍵証明証の情報が掲載されていないことを確認できたとしても、その最新のＣＲＬが発行されてから署名検証を行うまでの間に、対象公開鍵証明証が無効化されている可能性があり、署名検証を行った日時において、確かに署名検証に用いた公開鍵証明証が無効化されていないことを保証することができないという課題があった。

【０００５】上記の課題を図１０を用いて説明する。ＣＡにより時刻Ｔ１にＣＲＬが発行され、次回ＣＲＬ発行日時がＴ５である状況を想定する。この状況において、

時刻Ｔ２で利用者ＡがＣＡに対して公開鍵証明証の無効化申請を行い、その後、時刻Ｔ３に利用者Ａから例えばシステムＢに対してサービス申請が行われ、システムＢの署名検証装置において時刻Ｔ４に利用者Ａの署名検証が行われたとする。その際、システムＢの署名検証装置は署名検証に用いる公開鍵証明証が無効化されていないことを、時刻Ｔ１に発行されたＣＲＬを用いて確認するが、このＣＲＬでは、時刻Ｔ１以前に受け付けられた無効化証明証しか確認できず、時刻Ｔ２に無効化された公開鍵証明証の識別情報を確認することができないため、それを有効な公開鍵証明証であるとして署名検証を行い、その検証に合格すると、システムＢが利用者Ａにサービスを提供することになる。しかしながら、時刻Ｔ５に発行される新たなＣＲＬには、時刻Ｔ２で利用者Ａの公開鍵証明証が無効化されたことの情報が掲載されるため、時刻Ｔ４で行った署名検証は正しい処理でないことになる。

【０００６】

【課題を解決するための手段】上記に示した課題を解決するため、この発明では、署名検証を行う際に、これに用いる公開鍵証明証の無効化の有無を、次回のＣＲＬ発行日時以降に再度確認することにより、署名検証を行った日時において、確かに署名検証に用いた公開鍵証明証が無効化されていなかったことを保証する。まず図１に、この発明の機能構成を示し、構成要素である各手段を以下に説明する。

・公開鍵証明証有効性仮確認手段２１

署名検証処理時において、これに用いる公開鍵証明証の無効化の有無を確認し、無効化されていないことが確認された場合、状態管理テーブル２４にその公開鍵証明証の識別情報と、次回のＣＲＬ発行日時をその処理識別子と共に登録する。

・署名検証手段２２

公開鍵証明証を用いて依頼された署名検証処理を行い、署名検証がＯＫ（合格）であった場合に、状態管理テーブル２４に署名検証を行った日時を登録する。

・公開鍵証明証有効性確定手段２３

状態管理テーブル２４内に登録された公開鍵証明証の識別情報について、登録された次回ＣＲＬ発行日時以降に、その識別情報に対応する公開鍵証明証の署名検証日時の時点における、その公開鍵証明証の無効化の有無を確認し、最終的な署名検証結果を返却する。

・状態管理テーブル２４

署名検証を行った日時における、その検証に用いた公開鍵証明証の無効化の有無が確認可能となるまでの間、例えば図２に示すように署名検証処理ごとにその識別子を付け、その処理識別子と、その署名検証日時や、署名検証に用いた公開鍵証明証の識別情報、次回ＣＲＬ発行日時などの署名検証処理の状態を記憶して管理するテーブルである。

・更に時計２５を備え状態管理テーブル２４に対する読み書き消去は読み書き制御部２６により行う。

【０００７】次に、上記の各構成要素を用いた署名検証方法の流れを、図３を用いて説明する。

①例えばサービスを提供するシステム中のあるモジュールからの署名検証要求を受け付けると、公開鍵証明証有効性仮確認手段２１を用いて、署名検証に用いる公開鍵証明証が、既にＣＡによって無効化されていないことを確認し、無効化されていない場合、状態管理テーブル２４に対象公開鍵証明証の識別情報と、次回ＣＲＬ発行日時を登録する。すでに無効化されていることが確認された場合には、これを、署名検証要求元（この例ではシステムの前記モジュール）に通知して処理を終了する。

②①で署名検証に用いる公開鍵証明証の無効化が確認されなかった場合、署名検証手段２２により、システムのモジュールから依頼された署名検証処理を公開鍵証明証を用いて行い、検証ＯＫ（合格）であった場合、状態管理テーブル２４に署名検証を行った日時を登録する。また、検証ＮＧ（不合格）であった場合には、これを署名検証要求元（前記モジュール）に通知して処理を終了する。

③状態管理テーブル２４に登録した次回ＣＲＬ発行日時をシステム時刻（現在時刻）が過ぎた際に、公開鍵証明証有効性確定手段２３を用いて、状態管理テーブル２４内のその次回ＣＲＬ発行日時が登録されている識別情報に対応する公開鍵証明証が、署名検証日時の時点で無効化されていなかったことを確認する。ここで、再度無効化されていないことが確認された場合、検証ＯＫとともに状態管理テーブル２４に登録された署名検証日時情報を呼び出し元（署名検証要求モジュール）に通知する。無効化されていた場合には、検証ＮＧを呼び出し元に通知して処理を終了する。

【０００８】以上に示した処理方法を用いることにより、署名検証要求があった時に、その公開鍵証明証が無効化されていればそのことを署名検証要求元に直ちに通知することができ、また無効化されていないことにより、署名検証を行いそれが不合格の場合も、このことが直ちに通知される。更に署名検証処理を行った日時において、署名検証に用いた公開鍵証明証が確かに無効化されていなかったことを保証することが可能となる。また署名検証要求があった後、次のＣＲＬの発行を待って、その公開鍵証明証が無効化されていないことを確認して署名検証することも考えられるが、その前のＣＲＬで既に無効化されている場合や、署名検証に不合格となる場合に、これらの通知が遅れるが、この発明ではそのようなことがない。

【０００９】

【発明の実施の形態】この発明の実施例を図４乃至図７を用いて説明する。この実施例では、図４に示すように、ＣＡが新しいＣＲＬを毎日０時に発行する状況を想

定する。システムの署名検証装置が、利用者による公開鍵証明証の無効化依頼をＣＡに対し行う前に署名検証を行った場合（署名検証処理（１））と、無効化依頼後に署名検証を行った場合（署名検証処理（２））の両方において、この発明による署名検証処理の様子を、図５及び図６を用いて説明する。

【００１０】まず、２０００／５／１５の０時にＣＡから新たなＣＲＬが発行された後、システムＢが１０時に利用者Ａからの署名検証を伴うサービス申請（１）を受け付けたところを想定する。

Ｓ１．サービス申請（１）の受付処理に基づきそのモジュールから、署名検証装置の公開鍵証明証有効性仮確認手段２１が署名検証処理（１）の要求を受け付けると、まず、公開鍵証明証無効化確認機能を用いて、署名検証に用いる公開鍵証明証の無効化の有無を確認する。この時点で利用者Ａは無効化申請を行っていないため、利用者Ａの公開鍵証明証の無効化は確認されない。公開鍵証明証無効化確認機能は、自らがＣＲＬをＣＡから取得してＣＲＬの中身を確認する方法や、ＶＡへの問い合わせにより確認する方法が既に知られており、これらを利用することにより実現可能である。なお公開鍵証明証は利用者Ａがサービス申請時に送る場合、あるいはシステムＢが予めもっている場合などがあり、署名検証装置にはシステムＢから供給される。

【００１１】Ｓ２．Ｓ１の確認で無効化が確認されなかった場合、処理識別子、確認対象の公開鍵証明証の識別情報、次回ＣＲＬ発行日時情報を、テーブル登録機能を用いて状態管理テーブル２４に登録する。ここでは、図７に示すように処理識別子が「処理（１）」であり、確認対象の公開鍵証明証は、発行者名が「ＣＡ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」の公開鍵証明証であったこととしてこれらを登録するとともに、次回ＣＲＬ発行日時情報である「２０００／５／１６　０：００：００」も状態管理テーブル２４に登録する。テーブル登録機能は、例えば市販のＤＢシステムにおいてＤＢの情報を書き換えるためのＤＢ登録機能などが利用可能である。次回ＣＲＬ発行日時情報はＣＲＬ内にその情報が記載されておりこれを参照するか、ＶＡからの問い合わせ結果に一般に含まれており、その参照等により取得する。

【００１２】Ｓ３．次に、署名検証手段２２は、公開鍵証明証内から公開鍵を取り出し署名検証を行う。署名検証機能は、公開鍵、検証対象である電子署名、署名の生成対象である電子データを入力として電子署名の正当性の確認を行う機能であり、既存の暗号技術を用いて容易に実現可能である。

Ｓ４．Ｓ３の署名検証がＯＫであった場合、テーブル登録機能を用いて、署名検証日時情報を状態管理テーブル２４に登録する。ここでは、署名検証日時が「２０００／５／１５　１０：００：１０」であったこととして、これを図７に示すように処理（１）に対し登録する。なお署名検証が不合格であった場合は、そのことが署名検証要求元モジュールに直ちに通知され、また状態管理テーブル２４中の対応する処理識別子「処理（１）」の欄が消去される。

【００１３】ここで、サービス申請（１）の後で、利用者Ａによる公開鍵証明証の無効化申請がＣＡに対して行われ、その後、再度、利用者Ａからのサービス申請（２）を受け付けたところを次に想定する。

Ｓ５．サービス申請（２）の受付処理に基づき、署名検証装置の公開鍵証明証有効性仮確認手段２１が署名検証処理（２）の要求を受け付けると、Ｓ１と同様に、公開鍵証明証無効化確認機能を用いて、署名検証に用いる公開鍵証明証の無効化の有無を、最新のＣＲＬにより確認する。この時点で利用者Ａは既に無効化申請を行った後であるが、この時点でＣＲＬには、その情報はまだ掲載されていないため、システムＢの署名検証装置では、利用者Ａの公開鍵証明証の無効化は確認されない。

【００１４】Ｓ６．Ｓ５の確認で無効化が確認されなかったため、処理識別子、確認対象の公開鍵証明証の識別情報、次回ＣＲＬ発行日時情報を、テーブル登録機能を用いて状態管理テーブル２４に登録する。ここでは、図７に示すように処理識別子が「処理（２）」であり、確認対象の公開鍵証明証はＳ２のときと同様であったとし、次回ＣＲＬ発行日時情報である「２０００／５／１６　０：００：００」とともに状態管理テーブル２４に登録する。

【００１５】Ｓ７．次に、署名検証手段２２は、公開鍵証明証内から公開鍵を取り出し署名検証を行う。

Ｓ８．Ｓ７の署名検証がＯＫであった場合、テーブル登録機能を用いて、署名検証日時情報を状態管理テーブル２４に登録する。ここでは、署名検証日時が「２０００／５／１５　１３：００：１０」であったとして、これを図７に示すように処理（２）に対して登録する。

【００１６】続いて、図６に示すように次回ＣＲＬ更新日時である２０００／５／１６　０時を過ぎ、ＣＡから新たなＣＲＬが発行されたところを想定する。

Ｓ９．公開鍵証明証有効性確定手段２３は時計２５の現在時刻と状態管理テーブル２４内に登録済の次回ＣＲＬ発行日時とを比較し、現在時刻が次回ＣＲＬ発行日時を過ぎ、その新しいＣＲＬによる確認が可能な状態になると、状態管理テーブル２４に登録された各処理識別子に対応する情報の内、状態管理テーブル２４内に登録された次回ＣＲＬ発行日時が、システム時刻（現在時刻）より前の処理識別子の存在をテーブル参照機能により確認し、これら処理識別子のそれぞれについて、署名検証日時における公開鍵証明証の無効化の有無を、公開鍵証明証無効化確認機能を用いて確認する。つまりこの時点で最新のＣＲＬには、「２０００／５／１５　１１：００：００」に利用者Ａの公開鍵証明証（発行者名が「Ｃ

Ａ－１」、所有者名が「利用者Ａ」、通し番号が「１００１」）が無効化されていることの情報が掲載されているため、これにより図７に示した例では「処理（１）」の処理については、署名検証日時である「２０００／５／１５　１０：００：１０」の時点が無効化申請時刻より前であるから利用者Ａの公開鍵証明証は無効化されていなかったことが確認され、「処理（２）」の処理については、署名検証日時である「２０００／５／１５　１３：００：１０」の時点が無効化申請時刻より後であるから利用者Ａの公開鍵証明証は無効化されていたことが確認される。ここで利用されるテーブル参照機能は、例えば市販のＤＢシステムにおいてＤＢの情報を参照するためのＤＢ参照機能などが利用可能である。

【００１７】Ｓ１０．戻り値返却機能を用いて、署名検証要求モジュールにサービス申請（１）の処理については「署名検証ＯＫ」と「署名検証日時　２０００／５／１５１０：００：１０」を返却し、サービス申請（２）の処理については、「署名検証ＮＧ」を返却した後、テーブル削除機能を用いて、状態管理テーブル２４内の該当処理の情報を削除する。戻り値返却機能は、通常のプログラム作成において利用可能な機能であり、テーブル削除機能は、例えば市販のＤＢシステムにおいてＤＢの情報を削除するためのＤＢ削除機能などが利用可能である。

【００１８】上記のように、署名検証装置が署名検証を行う際、これに用いる公開鍵証明証の無効化の有無を、署名検証日時の時点における無効化の有無が確認可能となる次回ＣＲＬ発行日時以降に再度確認することにより、署名検証日時において確かに署名検証に用いた公開鍵証明証が無効化されていなかったことを保証した、正当な署名検証を行うことが可能となる。また署名検証要求を受けた際に、ＣＲＬによる公開鍵証明証の無効化の＊確認を行っているため、それが無効化されていれば、そのことが直ちに、要求元へ通知でき、更に無効化されていない場合は、その公開鍵証明証を用いて署名検証を行っており、その検証に不合格であれば、これが直ちに要求元へ通知される。

【００１９】上述した署名検証装置はその各手段を、コンピュータによりプログラムを実行させて機能させることもできる。

【００２０】

【発明の効果】この発明によれば、署名検証に用いた公開鍵証明証が、署名検証日時の時点で確実に無効化されていないことが確認されるため、データに付与された電子署名を検証し、さらにその検証した時刻を保証したサービスを提供することが可能となる。

【図面の簡単な説明】

【図１】この発明の装置の実施例の機能構成を示す図。

【図２】この発明のシステム状態管理テーブル２４の登録内容例を示す図。

【図３】この発明方法の処理の流れを実現する手段とアクセス資源を示す図。

【図４】実施例で想定するＣＲＬの発行や、公開鍵証明証の無効化申請、サービス申請等のタイミングを示す図。

【図５】図４の状況をもとに、この発明の実施例の処理の流れを示す図。

【図６】図５の処理の続きを示す流れ図。

【図７】図６に示した処理の流れの途中における状態管理テーブル内の様子の例を示す図。

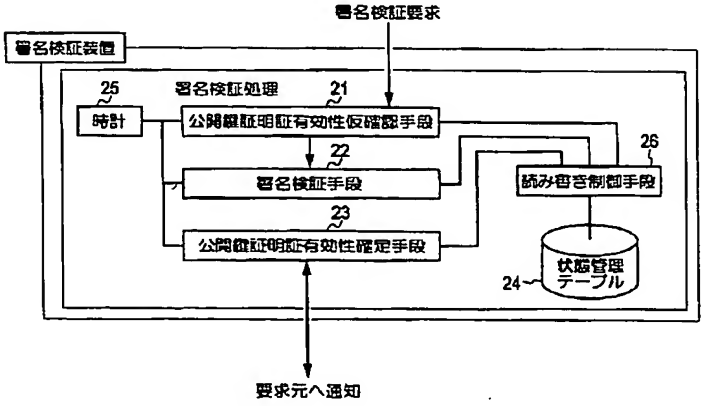
【図８】公開鍵証明証が無効にされていないかを確認するための手法を説明するための図。

【図９】その他の手段を説明するための図。

【図１０】この従来の問題点を説明するための図。

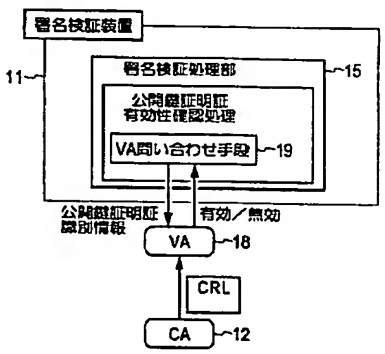
【図１】

図 1



【図９】

図 9



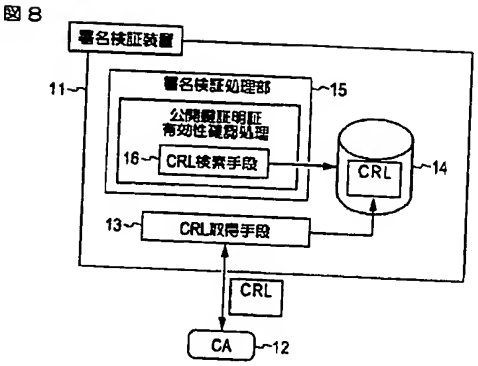
【図２】

図２

処理識別子	署名検証日時	公開鍵証明証識別情報	次回CRL発行日時
処理番号1	2000/05/15 10時20分00秒	公開鍵証明証1	2000/05/16 00時00分00秒
処理番号2	2000/05/15 13時00分00秒	公開鍵証明証2	2000/05/16 00時00分00秒
処理番号3	2000/05/15 20時00分00秒	公開鍵証明証3	2000/05/16 00時00分00秒

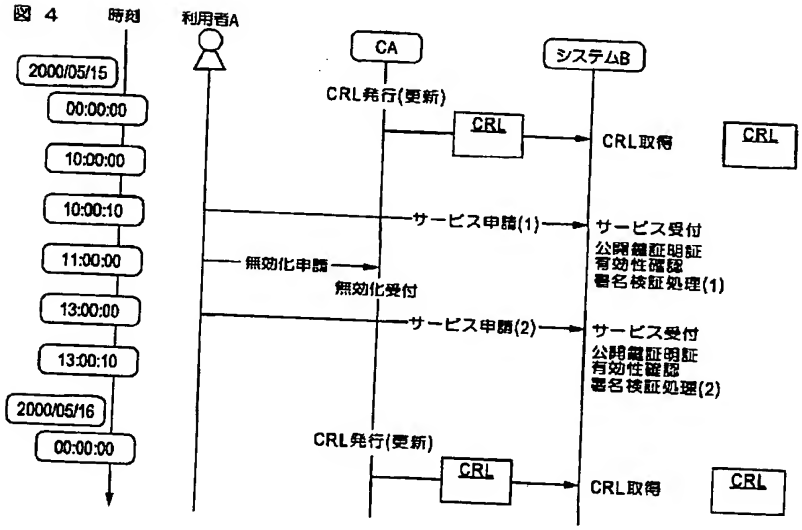
【図８】

図８



【図４】

図４



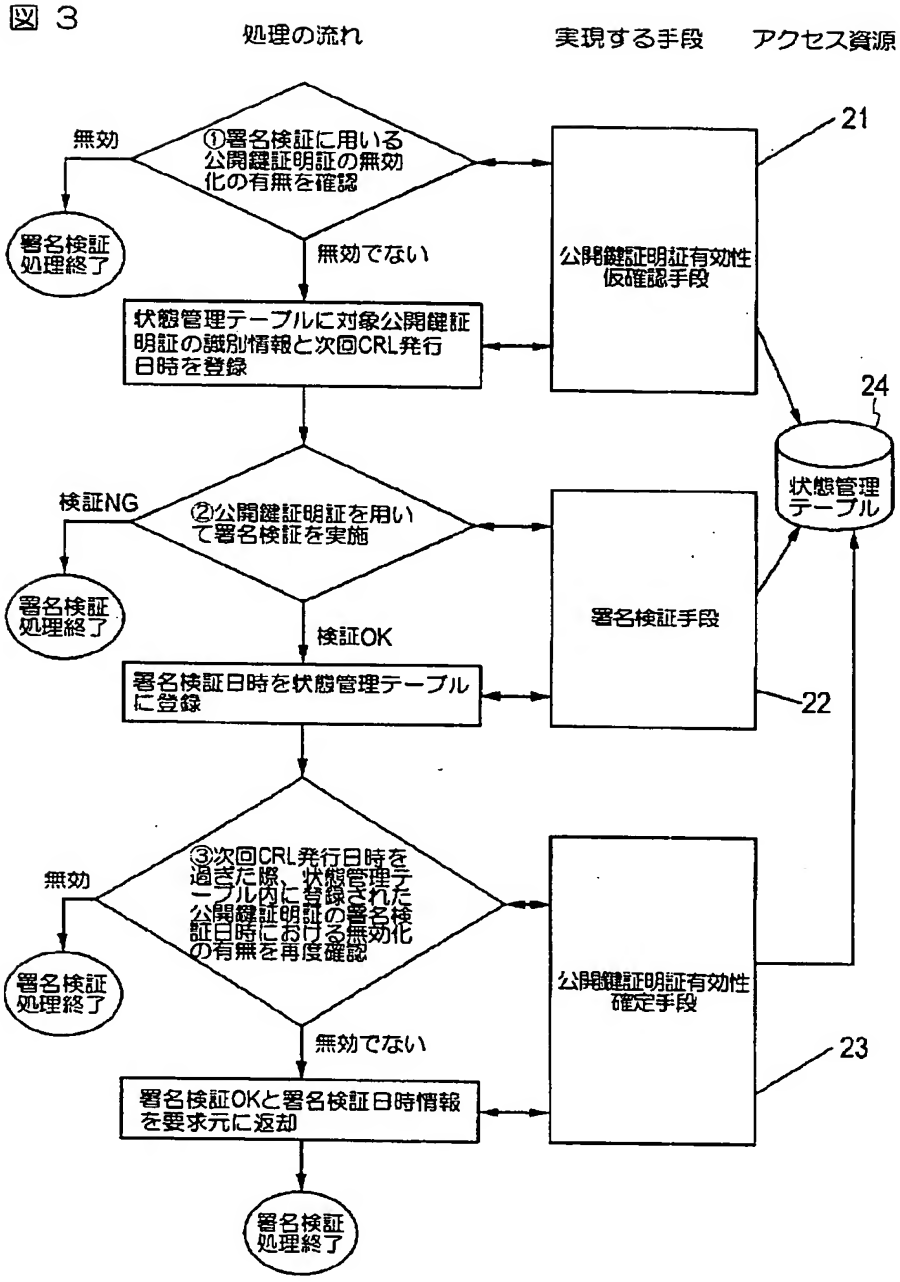
【図７】

図７

処理識別子	署名検証日時	公開鍵証明証識別情報			次回CRL発行日時
		発行者名	所有者名	シリアル番号	
処理(1)	2000/05/15 10:00:10	CA-1	所有者A	1001	2000/05/16 0:00:00
処理(2)	2000/05/15 13:00:10	CA-1	所有者A	1001	2000/05/16 0:00:00

【図３】

図 3


処理の流れ
実現する手段
アクセス資源
①署名検証に用いる公開鍵証明証の無効化の有無を確認
無効
署名検証処理終了
無効でない
公開鍵証明証有効性仮確認手段
21
状態管理テーブルに対象公開鍵証明証の識別情報と次回CRL発行日時を登録
24
状態管理テーブル
②公開鍵証明証を用いて署名検証を実施
検証NG
署名検証処理終了
検証OK
署名検証手段
署名検証日時を状態管理テーブルに登録
22
③次回CRL発行日時を過ぎた際、状態管理テーブル内に登録された公開鍵証明証の署名検証日時における無効化の有無を再度確認
無効
署名検証処理終了
無効でない
公開鍵証明証有効性確定手段
23
署名検証OKと署名検証日時情報を要求元に返却
署名検証処理終了

【図５】

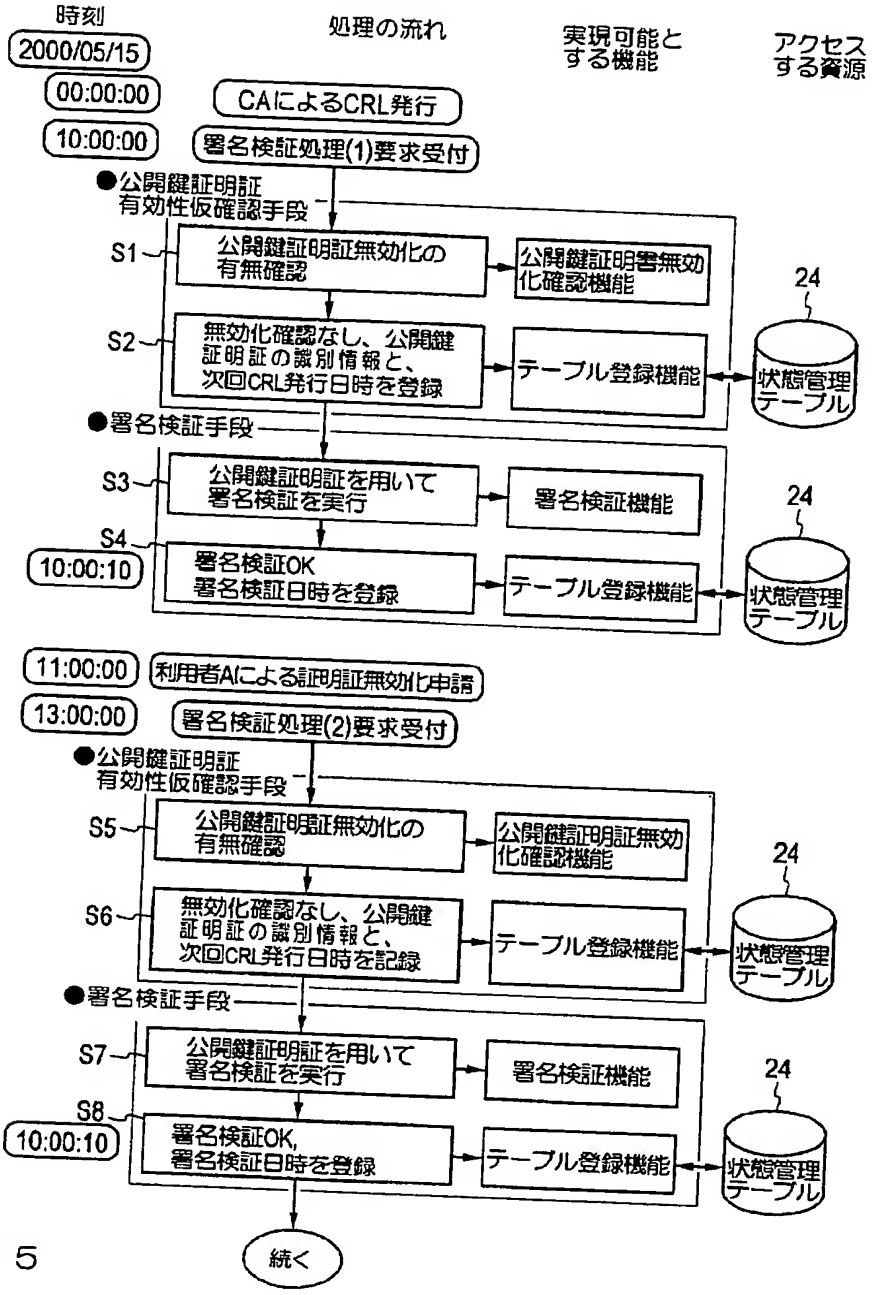

時刻
処理の流れ
実現可能とする機能
アクセスする資源
2000/05/15
00:00:00
CAによるCRL発行
10:00:00
署名検証処理(1)要求受付
●公開鍵証明証有効性仮確認手段
S1
公開鍵証明証無効化の有無確認
公開鍵証明書無効化確認機能
S2
無効化確認なし、公開鍵証明証の識別情報と、次回CRL発行日時を登録
テーブル登録機能
24
状態管理テーブル
●署名検証手段
S3
公開鍵証明証を用いて署名検証を実行
署名検証機能
S4
10:00:10
署名検証OK
署名検証日時を登録
テーブル登録機能
24
状態管理テーブル
11:00:00
利用者Aによる証明証無効化申請
13:00:00
署名検証処理(2)要求受付
●公開鍵証明証有効性仮確認手段
S5
公開鍵証明証無効化の有無確認
公開鍵証明証無効化確認機能
S6
無効化確認なし、公開鍵証明証の識別情報と、次回CRL発行日時を記録
テーブル登録機能
24
状態管理テーブル
●署名検証手段
S7
公開鍵証明証を用いて署名検証を実行
署名検証機能
S8
10:00:10
署名検証OK,
署名検証日時を登録
テーブル登録機能
24
状態管理テーブル
続く

図 5

【図６】

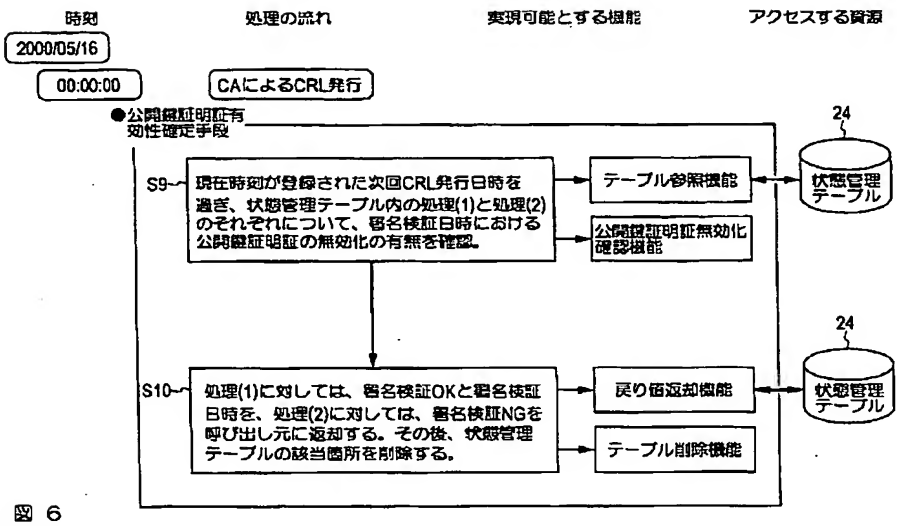
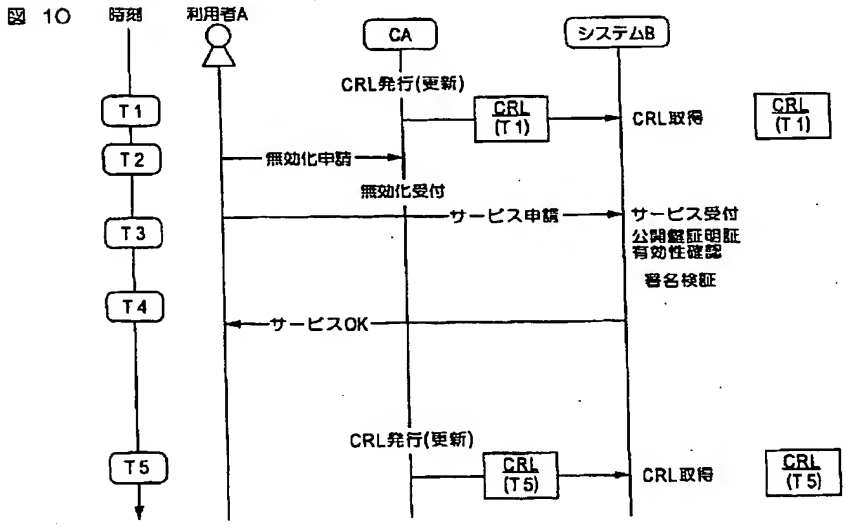


図 6

【図１０】



フロントページの続き

Ｆターム(参考) 5B049 AA05 CC31 DD05 EE05 EE09
FF09 GG10
5J104 AA09 AA16 EA05 LA03 LA06
NA02 PA07